X.9 4.176 Reference 4

(12) UK Patent Application (19) GB (11) 2 220 280 (13) A

(43) Date of A publication 04.01.1990

(21) Application No 8815897.7

(22) Date of filing 04.07.1988

(51) INT CL⁴
G05B 23/02 9/03

(52) UK CL (Edition J)
G3N NGK2 N287 N375 N381
U1S S1905

(56) Documents cited
None

(58) Field of search
UK CL (Edition J) G3N NGK1 NGK2
INT CL⁴ G05B

(71) Applicant
Rolls-Royce and Associates Limited
(Incorporated in the United Kingdom)
P.O. Box 31, Moor Lane, Derby, DE2 8BJ, United Kingdom

(72) Inventor
Christopher Rowland Line Spiller

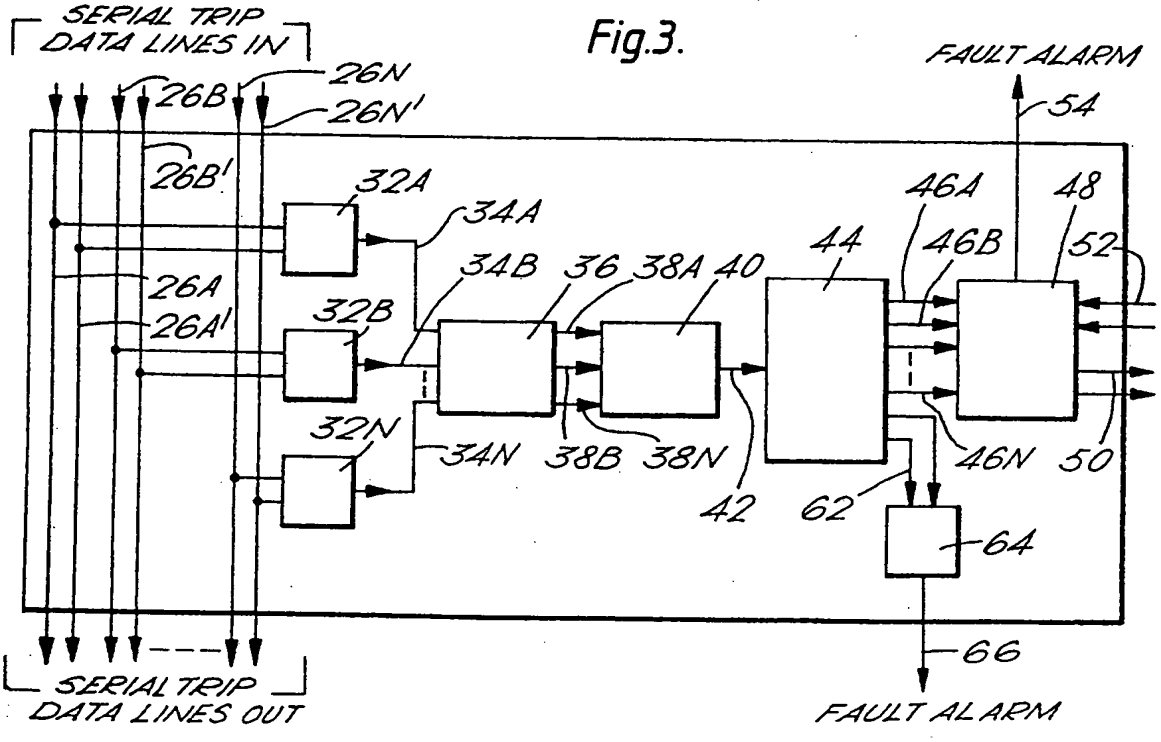
(74) Agent and/or Address for Service
M A Gunn
Rolls-Royce plc, Patents Department, PO Box 31, Moor Lane, Derby, DE2 8BJ, United Kingdom

(54) A control system for industrial plant

(57) A control system for an industrial plant eg. a pressurised water nuclear reactor, comprises a plurality of instrument sets and a plurality of logic sets (14A) etc. The instrument sets have a number of sensors which detect parameters (temperature, pressure vibration) of the industrial plant, and have two serial link controllers which supply the output signals from each sensor in the instrument set sequentially to the logic sets (14A) etc via conductors 26A, 26A', 26B, 26B' etc.

The logic sets have a number of auto select logic circuits (32A to 32N), each of which selects data from the sensors from one of the instrument sets, and a synchroniser (36) ensures that the output signals from the sensors detecting the same parameter are supplied to a voting logic circuit (40) at the same time. The voting logic circuit performs a voting function on the output signals to produce a series of high reliability signals which are converted to parallel high reliability signals by a series to parallel converter (44). The high reliability signals are supplied to a fault logic shutdown circuit (48) which controls the operation of shutdown mechanisms for the industrial plant.

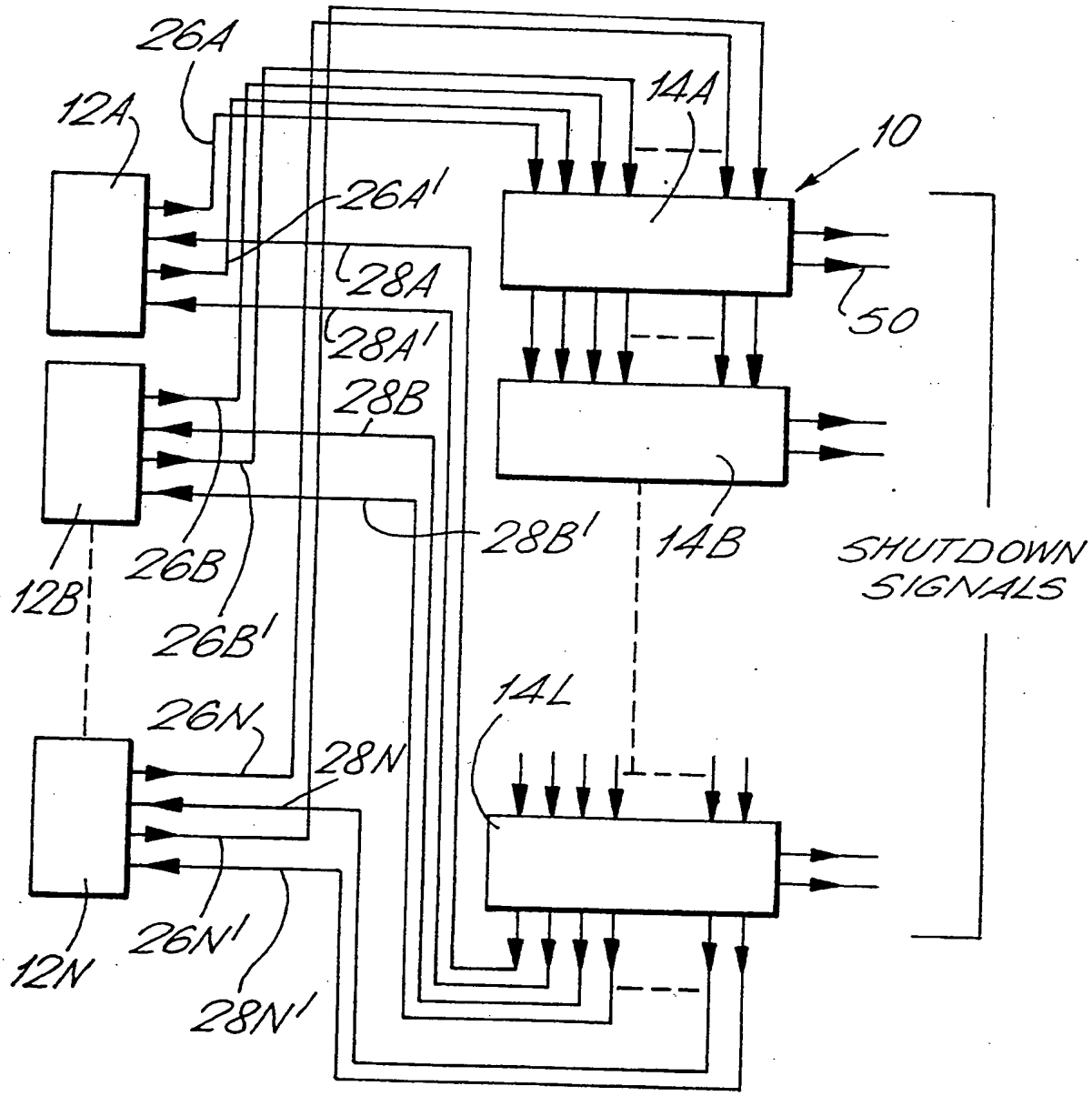
Fig.3.



GB 2 220 280 A

2220280

Fig.1.



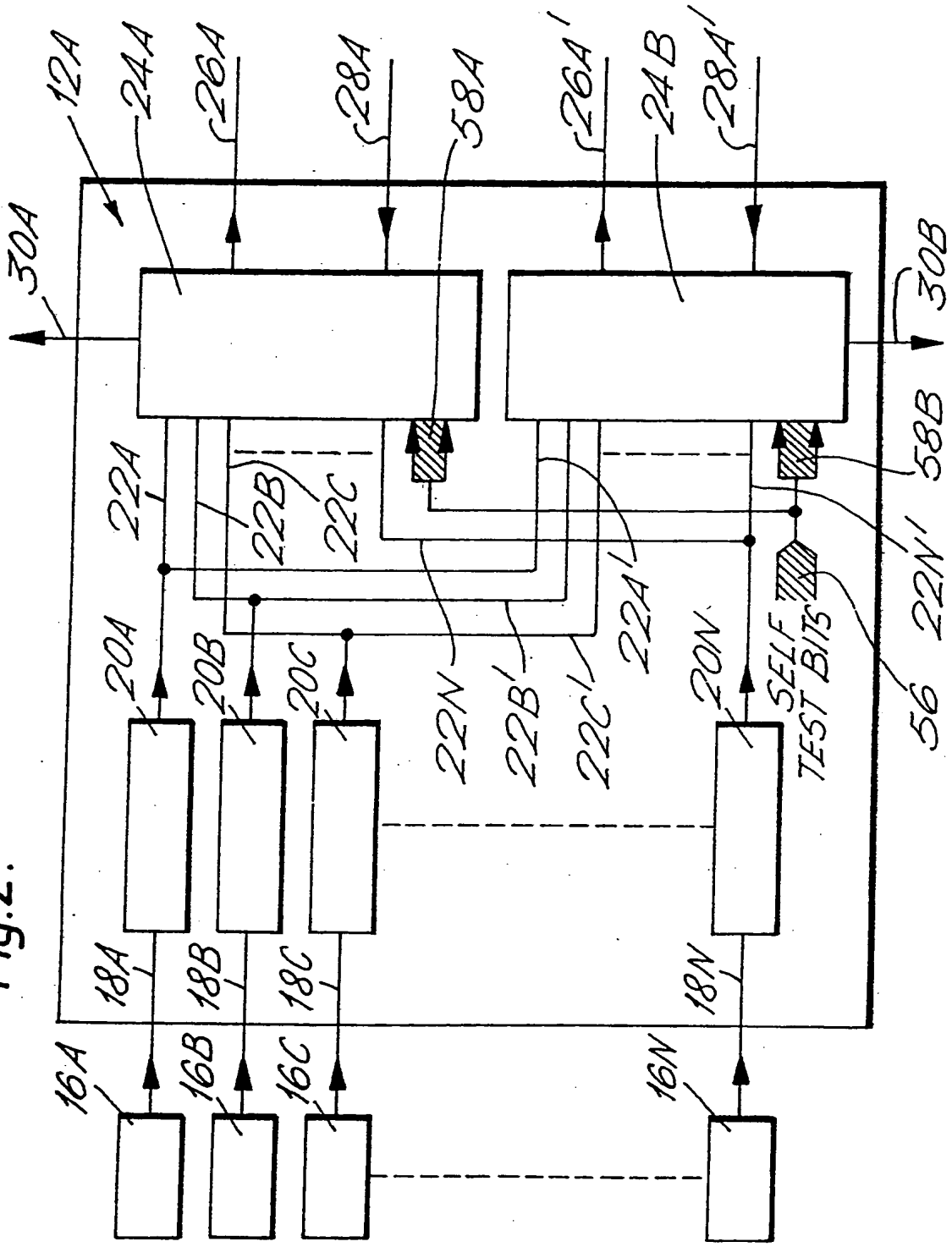


Fig.2.

2220280

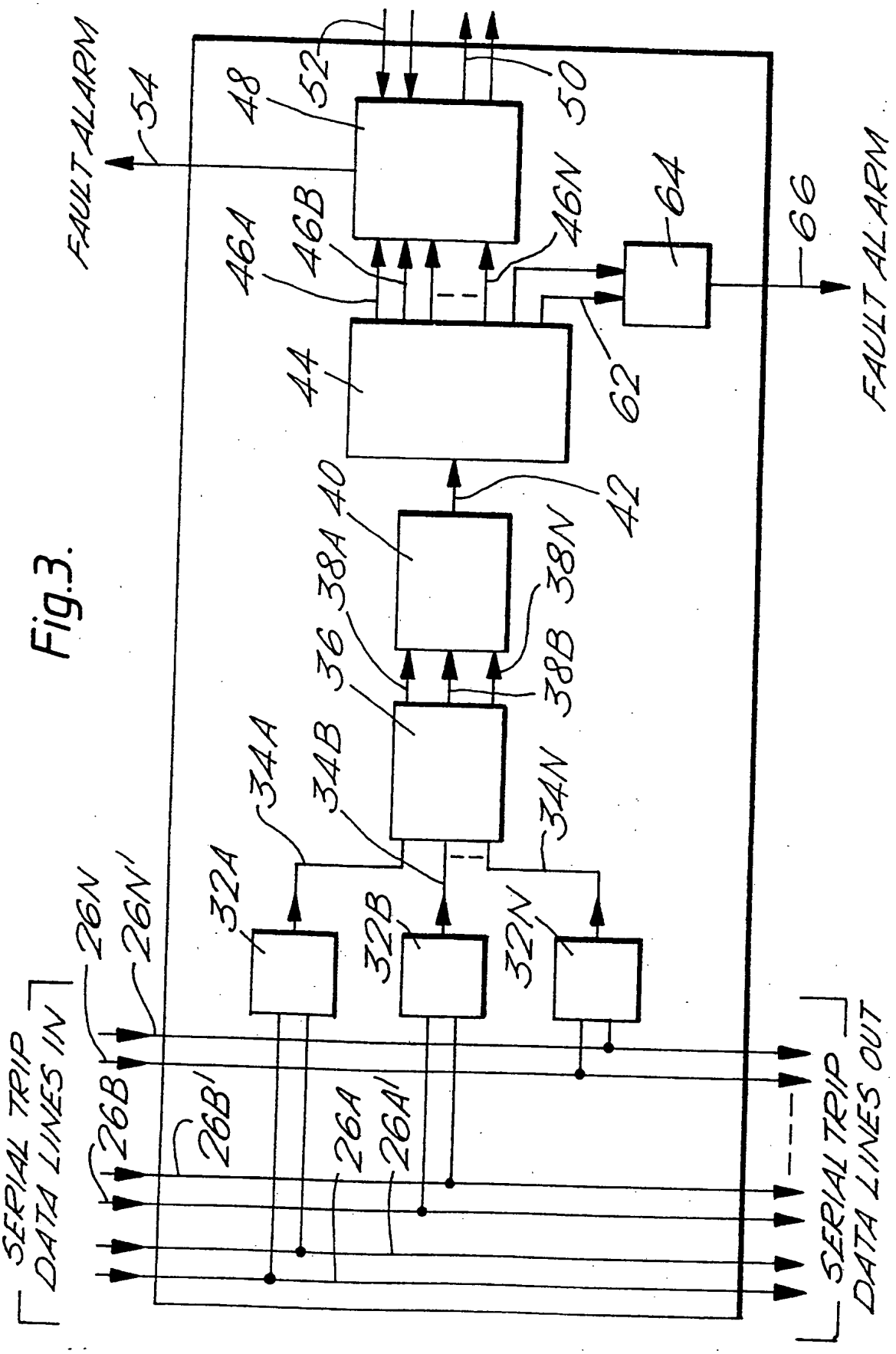


Fig.3.

2220280

Fig.4.

INSTRUMENT SET 1 TEST BITS	0 0 0 1 0 1 1 1
INSTRUMENT SET 2 TEST BITS	0 1 0 1 1 0 0 1
INSTRUMENT SET 3 TEST BITS	0 1 1 0 0 1 0 1
VOTING UNIT OUTPUT	0 1 0 1 0 1 0 1

VOTING UNIT SEES THE COMBINATIONS 000. 011. 001. ..... 111 IN SEQUENCE. AND SHOULD PRODUCE THE OUTPUT SHOWN.

A CONTROL SYSTEM FOR INDUSTRIAL PLANT

The present invention relates to control systems for Industrial Plant.

There is often a requirement in industrial plants for a control system which will shutdown the industrial plant, should the industrial plant operate outside a predetermined operating condition regime.

A known control system which will shutdown the industrial plant, should the industrial plant operate outside a predetermined operating regime, comprises a plurality of sensors which detect parameters of the industrial plant and which send output signals to a logic circuit which analyses the output signals to determine if the industrial plant is operating outside the predetermined operating regime. If the logic circuit determines that the industrial plant is operating outside the predetermined operating regime a shutdown signal is produced which is sent to some means for shutting down the industrial plant.

However, the consequences of a failure to shutdown the industrial plant when required, ie when the industrial plant is operating outside the predetermined operating regime, are very severe especially in some chemical plants or nuclear reactor power plants. This known control system is inadequate since a failure of any part of the control system may allow the industrial plant to continue operating when shutdown is required.

To overcome the problem of failure of any part of the control system described, improved control system comprising a number of sets of sensors, a number of logic circuits , and a voting logic circuit have been devised. In this control system each set of sensors sends their output signals to one of the logic circuits, which analyses the output signals to determine if the industrial plant is operating outside the predetermined operating regime. Each logic circuit sends a signal to the voting logic circuit. The voting logic circuit performs a function on the signals received from the logic circuits to produce a high

reliability shutdown signal. If any of the sensors, or logic circuits fail, the remaining sensors in other sets and logic circuits ensure that shutdown signals are sent to the voting logic circuit by some of the logic circuits.

However, the voting logic circuits are susceptible to failure, and in some industrial plant the failure probability of the voting logic circuit is still too high in terms of the probability of failure to shut down when required.

A further control system to overcome the problem of failure of the voting logic circuit, has used a number of voting logic circuits each of which receive the output signals from all the logic circuits. In this control system each voting logic circuit operates independent means for shutting down the industrial plant.

Such a control system provides an effective system with considerably reduced probability of failure to shut down the industrial plant when required. However, this control system uses a relatively large number of voting logic circuits and a relatively large number of connections, which makes the control system relatively bulky, relatively complex and relatively expensive.

The present invention seeks to provide a control system for an industrial plant which will shutdown the industrial plant, should the industrial plant operate outside a predetermined operating condition regime, with relatively low probability of failure and in which the control system is of reduced bulk, relatively simple and relatively cheap.

Accordingly the present invention provides a control system for an industrial plant comprising a plurality of instrument sets and a plurality of logic sets, each instrument set comprising a plurality of sensors to detect parameters of the industrial plant, each instrument set comprising a plurality of serial link controllers, each sensor being arranged to supply an output signal to each of the plurality of serial link controllers, each logic set comprising a plurality of auto select logic circuits, a synchroniser, a voting logic circuit, a serial to parallel

converter and a control logic circuit, each of the plurality of serial link controllers in each instrument set being arranged to supply the output signals from each of the sensors in the instrument set sequentially to one of the auto select logic circuits in each of the logic sets serially via respective transmission lines, each of the auto select logic circuits in each logic set being arranged to select data from the plurality of sensors from one of the instrument sets and being arranged to supply the data to the synchroniser, the synchroniser of each logic set being arranged to supply the data from each of the auto select logic circuits to the voting logic circuit of the logic set such that the output signals from the sensors in each instrument set detecting the same parameter are supplied to the voting logic circuit at substantially the same time, each voting logic circuit being arranged to perform a voting function on the output signals from the sensors in all the instrument sets detecting the same parameter to produce a series of single high reliability signals which are arranged to be supplied to the series to parallel converter of the logic set, each series to parallel converter being arranged to convert the series of high reliability signals to parallel high reliability signals which are supplied to the control logic circuit of the logic set, each control logic circuit being arranged to control the operation of an industrial plant in response to the high reliability signals.

The control logic may be a shutdown logic circuit arranged to control the operation of shutdown means for the industrial plant.

The control logic circuit may be a control algorithm processor circuit arranged to continuously control the industrial plant.

At least one of the auto select logic circuits may select data from the plurality of sensors from one of the instrument sets by selecting transmission lines with serial signals.

At least one of the auto select logic circuits may select data from the plurality of sensors from one of the instrument sets by selecting an error detecting coding.

The synchroniser may comprise a first in/first out memory.

The sequential output signals may be returned to the serial link controllers via respective second transmission lines for decoding and comparing with the transmitted output signals.

Each of the serial link controllers may have a fault alarm.

Each instrument set may comprise a self testing means, the self testing means being arranged to supply test signals to each of the plurality of serial link controllers, each serial link controller being arranged to supply the test signals sequentially with the output signals from each of the sensors in the instrument set to one of the auto select logic circuits in each of the logic sets serially via transmission lines, the voting logic circuit of each logic set being arranged to perform a voting function on the test signals from the self testing means of each instrument set to produce a high reliability test signal, each logic set having a checker means to ensure that the high reliability test signals is correct.

The checker means may receive signals from the series to parallel converter.

Each of the checker means may have a fault alarm.

The industrial plant may be a nuclear reactor plant.

The nuclear reactor plant may be a pressurised water nuclear reactor.

Each fault shutdown logic circuit may be arranged to control the operation of a separate shutdown means.

Each fault shutdown logic circuit may be arranged to control the operation of a single control rod or a group of control rods.

The present invention will be more fully described by way of example, with reference to the accompanying drawings, in which:-

Figure 1 is a schematic diagram of a control system for an industrial plant according to the present invention.

Figure 2 is a schematic diagram of an instrument set shown in Figure 1.

Figure 3 is a schematic diagram of a logic set shown in Figure 1.

Figure 4 is a table illustrating test vectors for a two out of three voting.

A control system 10 for an industrial plant (not shown) is shown in Figure 1 and comprises a plurality of instrument sets 12A, 12B to 12N and a plurality of logic sets 14A, 14B to 14L.

The instrument set 12A is shown schematically in more detail in Figure 2 and comprises a plurality of sensors 16A, 16B 16C to 16N, each of which detects a parameter, or condition, of the industrial plant. The sensors may measure for example temperatures, pressures, vibrations or any other required parameters at the same locations or different locations throughout the industrial plant. Each of the sensors 16A, 16B, 16C to 16N produces an output signal, dependent upon the parameter being detected, which is arranged to be supplied to respective instrument channels 20A, 20B, 20C to 20N via electrically conduction elements 18A, 18B, 18C to 18N respectively. The instrument channels 20A, 20B, 20C to 20N process the output signals, for example amplify, filter etc and produce trip signals. The instrument channels 20A, 20B, 20C to 20N are arranged to supply their respective output signals to a pair of serial link controllers 24A and 24B via electrically conducting elements 22A, 22B, 22C to 22N and 22A',22B',22C' to 22N' respectively. The instrument channels 20A to 20N also produce partial trip signals. Although two serial link controllers are used in the example, it may be equally possible to use more than two so as to increase the reliability of the control system. The serial link controllers 24A and 24B are arranged to transmit the output signals from each of sensors 16A, 16B, 16C to 16N serially to each of the logic sets 14A, 14B to 14L via electrically conducting elements 26A and 26A' respectively which connect

the logic sets 14A to 14L in series. Electrically conducting elements 28A and 28A' return the output signals to the serial link controllers 24A and 24B for checking that the output signals received by the logic sets are in accordance with the output signals transmitted. If a discrepancy is detected the serial link controllers cease transmission, if there is a presence of serial signals these are used by the logic sets. The serial link controllers 24A and 24B are electrically connected by elements 30A and 30B to fault alarms (not shown) for the supplying of a fault alarm signal to operate the fault alarm if a discrepancy is detected by the serial link controllers 24A and 24B between the output signals transmitted, and the output signals received by the logic sets.

The instrument sets 12B, 12C to 12N are substantially the same as instrument set 12A, and the instrument sets 12B, 12C to 12N will have sensors measuring the same parameters at the same locations as instrument set 12A. However, some of the instrument sets may not have all the sensors, if the sensors measuring a particular parameter are sufficiently reliable to require fewer copies than there are instrument sets. Where a sensor is omitted its output line is tied to a trip or non-trip state, as required to obtain the desired voting from the sensors which are present.

The serial link controllers may use any suitable protocols such as error detecting coding for example a hamming type coding scheme or cyclic redundancy check.

The logic set 14A is shown schematically in more detail in Figure 3 and comprises a plurality of auto select logic circuits 32A, 32B to 32N, ie one auto select logic circuit for each instrument set, and each of the auto select logic circuits 32A, 32B to 32N is arranged to select the output signals from all of the sensors from one of the instrument sets by selecting an electrically conducting element with serial signals/or by avoiding a conducting element not having serial signals. Therefore, for example the auto select logic circuit 32A selects the output signals from all of the sensors 16A, 16B, 16C to 16N from instrument set 12A from conducting element 26A or 26A'. Similarly auto select

logic circuit 32B selects the output signals from all of the sensors from instrument set 12B from conducting element 26B or 26B'. Likewise auto select logic circuits 32C to 32N select the output signals from all the sensors in sets 12C to 12N.

If hamming type coding scheme is used, a code checker is used in the selection logic.

The auto select logic circuits 32A to 32N are arranged to supply data, ie the selected output signals, to the synchroniser 36, and the synchroniser 36 ensures that the output signals from the sensor in each instrument set detecting the same parameter are supplied to the voting logic circuit 40 at substantially the same time via electrically conducting elements 38A to 38N respectively. The synchroniser 36 may comprise a first in/first out memory.

The voting logic circuit 40 is arranged to perform a voting function on the output signals from the sensors in all the instrument sets detecting the same parameter, and the voting function is performed for the output signals from the sensors in all the instrument sets for all the parameters in sequence to produce a single serial high reliability signal. The single serial high reliability signal is supplied to a series to parallel converter 44 via an electrically conducting element 42, the series to parallel converter 44 is arranged to convert the single serial high reliability signal to parallel high reliability signals which are supplied to a fault shutdown logic circuit 48 via electrically conducting elements 46A to 46N.

The fault shutdown logic circuit 48 is arranged to control the operating of a shutdown mechanism for the industrial plant in response to the high reliability signals by supplying shutdown output signals via elements 50.

The logic sets 14B to 14L are substantially the same and operate in substantially the same manner as instrument set 14A.

The shutdown logic is designed to give the shutdown output signals in one out of two, two out of three, two out of four, three out of four or other suitable codes. The

shutdown output signals are looped back by elements 52 and checked, so as to check both the shutdown logic and the output connection elements 50. If a fault is detected by this checking a fault alarm signal is supplied to a fault alarm (not shown) by electrical connection elements 54 to operate the fault alarm to initiate maintenance. The shutdown logic circuit 48 also incorporates error detecting codes in addition to the loop back checking.

The instrument set 12A has a self test system 56 which supplies test signals to the serial link controllers 24A and 24B via electrical connector elements 58A and 58B respectively. The serial link controllers 24A, 24B supplies the test signals sequentially with the output signals from the sensors, in the instrument set, to one of the auto select logic circuits in each of the logic sets. The test signals are processed by the synchroniser, voting logic circuit and series to parallel converter. The logic set 14A has a checker circuit 64 which receives the test signal by electrical connector elements 62 from the series to parallel converter 44. The checker circuit 64 has an electrical connection element 66 which supplies a fault alarm signal to a fault alarm (not shown).

If the auto-select logic circuits base their decision on the presence of serial signals, it is necessary for the serial link controllers to cease transmission if a fault is detected.

All of the instrument sets 12B to 12N also have self test systems, and all of the logic sets 14B to 14L have checker circuits.

The self test systems in the different instrument sets are arranged to transmit different test signals so that when they arrive at the voting logic circuits they form a set of test vectors. The checker circuits check that the voting logic circuits response to the test vectors is correct after conversion to parallel form, and if it is incorrect a fault alarm signal is sent to the fault alarm to initiate maintenance. An example of test signals is shown in Figure 4 for a two out of three voting system. The voting logic

circuits should receive the combination of test signals, from the self test systems of three instrument sets of 001, 011, 001 .... 111 in sequence and produce the outputs 0, 1, 0 .... 1, the checker circuit checks that this is achieved.

The control system has individual parameter voting, and allows the flexibility to tailor the degree of redundancy of each individual sensor and channel. The control system incorporates self testing features which enables faults in the most sensitive area to be self announcing, this reduces the probability of system failure by reducing the fault detection time. Redundancy at individual sensor and channel rather than instrument set also reduces the probability of control system failure to produce an extremely reliable control system.

The control system has voting performed on individual parameter rather than on a guard line basis as in the prior art. A further advantage of the control system is that parameter voting is achieved with the number of logic sets being a function of the number of independent output signals required rather than of the number of parameters being measured.

The control system described is particularly suitable for use with nuclear reactor plant, for example pressurised water nuclear reactors (PWR). In such a control system the shutdown output signals from the logic sets would be supplied to separate control rods, or a small group of control rods, such that a failure of one logic set or one control rod could neither cause shutdown nor prevent shutdown, due to the limited effect of a single control rod or small group of control rods.

The control system may be used to shutdown the nuclear reactor plant using other methods.

The invention has been described by way of reference to a shutdown logic circuit, but any suitable control logic circuit may be used, for example the shutdown logic circuit may be replaced by a control algorithm processor circuit in the event that continuous control of the industrial plant is required rather than a shutdown control.

The control system is equally suitable for use with other industrial plant e.g. hazardous chemical plants.

In the control system for use with the nuclear reactor plant the output signals from the sensors are trip states, whereas in the control system for use with other industrial plant the output signals from the sensors may be levels. The voting logic circuit for other industrial plant is arranged to reject wild output signals and to produce a high reliability best estimate signal from those available.

Claims:-

1. A control system for an industrial plant comprising a plurality of instrument sets and a plurality of logic sets, each instrument set comprising a plurality of sensors to detect parameters of the industrial plant, each instrument set comprising a plurality of serial link controllers, each sensor being arranged to supply an output signal to each of the plurality of serial link controllers, each logic set comprising a plurality of auto select logic circuits, a synchroniser, a voting logic circuit, a serial to parallel converter and a control logic circuit, each of the plurality of serial link controllers in each instrument set being arranged to supply the output signals from each of the sensors in the instrument set sequentially to one of the auto select logic circuits in each of the logic sets serially via respective transmission lines, each of the auto select logic circuits in each logic set being arranged to select data from the plurality of sensors from one of the instrument sets and being arranged to supply the data to the synchroniser, the synchroniser of each logic set being arranged to supply the data from each of the auto select logic circuits to the voting logic circuit of the logic set such that the output signals from the sensors in each instrument set detecting the same parameter are supplied to the voting logic circuit at substantially the same time, each voting logic circuit being arranged to perform a voting function on the output signals from the sensors in all the instrument sets detecting the same parameter to produce a series of single high reliability signals which are arranged to be supplied to the series to parallel converter of the logic set, each series to parallel converter being arranged to convert the series of high reliability signals to parallel high reliability signals which are supplied to the control logic circuit of the logic set, each control logic circuit being arranged to control the operation of the industrial plant in response to the high reliability signals.

2. A control system as claimed in claim 1 in which the

control logic circuit is a shutdown logic circuit arranged to control the operations of shutdown means for the industrial plant.

3. A control system as claimed in claim 1 in which the control logic circuit is a control algorithm processor circuit arranged to continuously control the industrial plant.

4. A control system as claimed in any of claims 1 to 3 in which at least one of the auto select logic circuits selects data from the plurality of sensors from one of the instrument sets by selecting transmission lines with serial signals.

5. A control system as claimed in any of claims 1 to 3 in which at least one of the auto select logic circuits selects data from the plurality of sensors from one of the instrument sets by selecting an errror detecting coding.

6. A control system as claimed in any of claims 1 to 5 in which the synchroniser comprises a first in/first out memory.

7. A control system as claimed in any of claims 1 to 6 in which the sequential output signals are returned to the serial link controllers via respective second transmission lines for decoding and comparing with the transmitted output signals.

8. A control system as claimed in claim 7 is which each of the serial link controllers has a fault alarm.

9. A control system as claimed in any of claims 1 to 8 in which each instrument set comprises a self testing means, the self testing means being arranged to supply test signals to each of the plurality of serial link controllers, each serial link controller being arranged to supply the test signals sequentially with the output signals from each of the sensors in the instrument set to one of the auto select logic circuits in each of the logic sets serially via transmission lines, the voting logic circuit of each logic set being arranged to perform a voting function on the test signals from the self testing means of each instrument set to produce a high reliability test signal, each logic set

having a checker means to ensure that the high reliability test signals is correct.

10. A control system as claimed in claim 9 in which the checker means receives signals from the series to parallel converter.

11. A control system as claimed in claim 9 or claim 10 in which each of the checker means has a fault alarm.

12. A control system as claimed in any of claims 1 to 11 in which each fault shutdown logic circuit is arranged to control the operation of a separate shutdown means.

13. A control system as claimed in any of claims 1 to 11 in which the industrial plant is a nuclear reactor plant.

14. A control system as claimed in claim 13 in which the nuclear reactor plant is a pressurised water nuclear reactor.

15. A control system as claimed in claim 13 or claim 14 in which each fault shutdown logic circuit is arranged to control the operation of a single control rod or a group of control rods.

16. A control system for an industrial plant substantially as hereinbefore described with reference to and as shown in the accompanying drawings.

Published 1989 at The Patent Office, State House, 66-71 High Holborn, London WC1R 4TP Further copies may be obtained from The Patent Office, Sales Branch, St Mary Cray, Orpington, Kent BR5 3RD Printed by Multiplex techniques ltd, St Mary Cray, Kent, Con. 1/87

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2-73403

⑤Int. Cl.⁵	識別記号	庁内整理番号
G 05 B 9/02	B	6728-5H
G 21 D 3/04	GDP	7808-2G

⑬公開　平成2年(1990)3月13日

審査請求　未請求　請求項の数 15　(全8頁)

⑤④発明の名称　工業プラント用制御システム

⑳特　願　平1-172850
㉒出　願　平1(1989)7月4日
優先権主張　㉜1988年7月4日㉝イギリス(GB)㉛8815897.7

⑦②発明者　クリストファー・ローランド・ライン・スピラー　イギリス国ダービー，リトルオーバー，ラチニールド・ウエイ　22
⑦①出願人　ロールスーロイス・アンド・アソシエイツ・リミテツド　イギリス国ダービー　デイーイー2・8ビージエイ，ムーア・レーン(番地なし)
⑦④代理人　弁理士　湯浅　恭三　外4名

明　細　書

1.〔発明の名称〕

工業プラント用制御システム

2.〔特許請求の範囲〕

1.　複数の機器セットと複数の論理回路セットとを備える工業プラント用制御システムにおいて、

それぞれの機器セットは、工業プラントのパラメータを検出する複数のセンサと複数のシリアル・リンク制御器とを備え、

それぞれのセンサは、複数のシリアル・リンク制御器のそれぞれに出力信号を供給するようになされ、

それぞれの論理回路セットは、複数の自動選択論理回路と、同期装置と、議決論理回路と、直列－並列変換器と、制御論理回路とを有し、

それぞれの機器セットにおける複数のシリアル・リンク制御器のそれぞれは、機器セットにおける各センサからの出力信号を順次にそれぞれの伝送線を介してシリアルに論理回路セットのそれぞれにおける自動選択論理回路に供給するようになされ、

それぞれの論理回路セットにおける自動選択論理回路のそれぞれは、機器セットの1つから複数のセンサからのデータを選択し、該データを同期装置に供給するようになされ、

それぞれの論理回路セットの同期装置は、同一のパラメータを検出する各機器セットのセンサからの出力信号が実質的に同時に議決論理回路に供給されるように、自動選択論理回路のそれぞれからのデータを論理回路セットの議決論理回路へ供給するようになされ、

それぞれの議決論理回路は、同一のパラメータを検出する全ての機器セットのセンサからの出力信号に対して議決機能を遂行して、論理回路セットの直列－並列変換器へ供給される単一の高信頼性信号の列を出力するようになされ、

それぞれの直列－並列変換器は、高信頼性信号の列を論理回路セットの制御論理回路へ供給される並列の高信頼性信号へ変換するようになされ、

それぞれの制御論理回路は、高信頼性信号に応

答して工業プラントの動作を制御するようになされている
制御システム。

2. 制御論理回路が、工業プラント用操業停止手段の作動を制御するようにされた停止論理回路である請求項1記載の制御システム。

3. 制御論理回路が、工業プラントを連続的に制御するようになされた制御アルゴリズム・プロセッサである請求項1記載の制御システム。

4. 少なくとも1つの自動選択論理回路が、シリアル信号を伴う伝送線を選択することによって、機器セットの1つから複数のセンサからのデータを選択する請求項1記載の制御システム。

5. 少なくとも1つの自動選択論理回路が、誤り検出符号を選択することによって、機器セットの1つから複数のセンサからのデータを選択する請求項1記載の制御システム。

6. 同期装置が先入れ先出し記憶装置である請求項1記載の制御システム。

7. 順次の出力信号が、それぞれの第2の伝送線を介してシリアル・リンク制御器へ戻され、複号されて、送信された出力信号と比較される請求項1記載の制御システム。

8. シリアル・リンク制御器のそれぞれが故障警報器を有する請求項7記載の制御システム。

9. それぞれの機器セットが自己試験手段を含み、該自己試験手段は試験信号を複数のシリアル・リンク制御器のそれぞれに供給するようになされ、それぞれのシリアル・リンク制御器は機器セットの各センサからの出力信号と共に順次に試験信号を伝送線を介してそれぞれの論理回路セットの自動選択論理回路の1つにシリアルに供給するようになされ、論理回路セットのそれぞれの議決回路は機器セットのそれぞれの自己試験手段からの試験信号に対して議決機能を遂行して高信頼性試験信号を生成するようになされ、それぞれの論理回路セットは高信頼性試験信号が正しいことを保証するチェッカー手段を有する請求項1記載の制御システム。

10. チェッカー手段が直列ー並列変換器から信号を受け取る請求項9記載の制御システム。

11. それぞれのチェッカー手段が故障警報器を有する請求項9記載の制御システム。

12. それぞれの故障停止論理回路が個別の停止手段の動作を制御するようになされた請求項1記載の制御システム。

13. 工業プラントが原子炉プラントである請求項1記載の制御システム。

14. 原子炉プラントが加圧水型原子炉である請求項13記載の制御システム。

15. それぞれの停止論理回路が単一の制御棒又は一群の制御棒の動作を制御する請求項13記載の制御システム。

3.〔発明の詳細な説明〕

(産業上の利用分野)

本発明は、工業プラント用の制御システムに関する。

(従来の技術)

工業プラントが所定の作動条件レジーム(operating condition vegime)の範囲外で作動するような場合に、工業プラントを停止させる制御システムに対する要求が工業プラントには存在することが多い。

工業プラントが所定の作動条件レジームの範囲外で作動するときに工業プラントを停止させる公知の制御システムは、工業プラントのパラメータを検出し、出力信号を論理回路へ送る複数のセンサを備え、該論理回路は前記出力信号を分析して、工業プラントが所定の作動レジーム外で作動しているかどうかを決定する。工業プラントが所定の作動レジーム外で作動していると論理回路が決定するならば、停止信号が生成されて、工業プラントの操業を停止させるためのある種の手段へ送出される。

しかしながら、必要なときに、即ち、工業プラントが所定の作動レジーム外で作動しているときに工業プラントを停止させそこなった結果は、特に化学プラントや原子力発電所では悲惨である。この公知の制御システムは、制御システムの何等かの部分の不首尾により、操業停止が必要なとき

に工業プラントの作動を継続させることになる。

制御システムの何等かの部分の不首尾という上記の問題を克服するために、複数組のセンサと複数の論理回路と議決(voting)論理回路とを備える改良された制御システムが考案された。この制御システムでは、各組のセンサがその出力信号を論理回路の1つへ送り、その1つの論理回路が前記出力回路を分析して工業プラントは所定の作動レジーム外で作動しているかどうかを決定する。各論理回路は信号を議決論理回路へ送出する。議決論理回路は、論理回路から受け取った信号に作用を及ぼして高信頼度の停止信号を生成する。例えいずれかのセンサ又は論理回路が役に立たなくても、他の組の残りのセンサ及び論理回路により、いくつかの論理回路が操業停止信号を議決論理回路へ送ることが保証される。

しかしながら、議決論理回路が役に立たなくなる可能性があり、ある種の工業プラントでは、議決論理回路の動作不良の可能性は、必要なときに操業停止がなされない可能性に関して極めて高い。

議決論理回路の動作不良という問題を克服する別の制御システムは、全ての論理回路からの出力信号をそれぞれが受け取る複数の議決論理回路を用いている。この制御システムでは、それぞれの議決論理回路は、工業プラントを停止させるための独立の手段を作動させる。

こうした制御システムは、必要なときに工業プラントの操業を停止させそこなう可能性を大巾に減少させた有効なシステムである。しかしながら、この制御システムは比較的多くの数の議決論理回路と比較的多くの接続部とを使用するので、制御システムが大型化し、比較的複雑且つ高価になってしまう。

(発明が解決しようとする課題)

本発明は、工業プラントが所定の作動条件レジーム(regime)の範囲外で作動する場合に、比較的低い故障確率で工業プラントの操業を停止させ、しかも小型化され比較的簡単で比較的安価な工業プラント用制御システムを指向する。

(課題を解決するための手段)

したがって、本発明は、複数の機器セットと複数の論理回路セットとを有する工業プラント用制御システムを提供する。それぞれの機器セットは工業プラントのパラメータを検出する複数のセンサと複数のシリアル・リンク制御器とを備え、それぞれのセンサは複数のシリアル・リンク制御器のそれぞれに出力信号を供給するようになされ、それぞれの論理回路セットは複数の自動選択論理回路と、同期装置と、議決論理回路と、直列ー並列変換器と、制御論理回路とを備え、それぞれの機器セットの複数のシリアル・リンク制御器のそれぞれは、機器セットのそれぞれのセンサからの出力信号をシリアルにそれぞれの伝送線を介してそれぞれの論理回路セットの自動選択論理回路の1つに順次供給するようになされ、それぞれの論理回路セットの自動選択論理回路のそれぞれは機器セットの1つから複数のセンサからのデータを選択し、このデータを同期装置に供給するようになされ、それぞれの論理回路セットの同期装置は、同一のパラメータを検出するそれぞれの機器セットのセンサからの出力信号が実質的に同時に議決論理回路に供給されるように、自動選択論理回路のそれぞれからのデータを論理回路セットの議決論理回路に供給するようになされ、それぞれの議決論理回路は、同一のパラメータを検出する全ての機器セットにおけるセンサからの出力信号に対して議決機能を遂行して、論理回路セットの直列ー並列変換器に供給されるべき単一の高信頼性信号の列を生成するようになされ、それぞれの直列ー並列変換器は高信頼性信号の列を、論理回路セットの制御論理回路に供給される並列の高信頼性信号へ変換するようになされ、それぞれの制御論理回路は高信頼性信号に応答して工業プラントの動作を制御するようになされている。

制御論理回路は、工業プラント用操業停止手段の動作を制御する停止論理回路であってよい。

制御論理回路は、工業プラントを連続的に制御する制御アルゴリズム・プロセッサ回路であってよい。

少なくとも1つの自動選択論議回路は、シリア

ル信号で伝送線を選択することによって、機器セットの1つから複数のセンサからのデータを選択しうる。

少なくとも1つの自動選択論理回路は、誤り検出符号を選択することによって、機器セットの1つから複数のセンサからのデータを選択しうる。

同期装置は先入れ先出し記憶装置を含みうる。

順次の出力信号はそれぞれの第2の伝送線を介してシリアル・リンク制御器に戻され、復号されて、送信された出力と比較される。

それぞれのシリアル・リンク制御器は故障警報器を有してよい。

それぞれの機器セットは自己試験手段を備えうる。自己試験手段は複数のシリアル・リンク制御器のそれぞれに試験信号を供給するようになされ、それぞれのシリアル・リンク制御器は、機器セットのそれぞれのセンサからの出力信号と共に順次に試験信号を伝送線を介してシリアルに論理回路セットのそれぞれの自動選択論理回路の1つに供給するようになされ、それぞれの論理回路セットの議決論理回路は、それぞれの機器セットの自己試験手段からの試験信号に議決機能を遂行して高信頼性信号を生成するようになされ、それぞれの論理回路セットは高信頼性信号が正しいことを保証するチェッカー手段を有する。

チェッカー手段は直列－並列変換器から信号を受け取り得る。

それぞれのチェッカー手段は故障警報器を備えうる。

工業プラントは原子炉プラントであってよい。

原子炉プラントは加圧水型原子炉であってよい。

それぞれの故障停止論理回路は、個別の操業停止手段の動作を制御するようになされうる。

それぞれの故障停止論理回路は、単一の制御棒又は一群の制御棒の動作を制御するようになされうる。

本発明は、添付の図面を参照しながら例を用いて一層詳細に説明される。

（実施例）

工業プラント（図示せず）用制御システム10が第1図に図示され、複数の機器セット(instrument sets)12A,12B,…,12N及び複数の論理回路セット(logic sets)14A,14B,…,14Lを備えている。

機器セット12Aは第2図に詳細に図示され、複数のセンサ16A,16B,16C,…,16Nを含み、各センサは工業プラントのパラメータ即ち状態を検出する。これらセンサは工業プラント全域での同一位置又は異なる位置で、例えば温度，圧力，振動その他の必要なパラメータを測定する。センサ16A,16B,16C,…,16Nの各々は、検出中のパラメータに依存する出力信号を生成し、この出力信号はそれぞれ導電要素18A,18B,18C,…,18Nを介して各々の機器チャンネル20A,20B,20C,…,20Nに供給されるようになされている。機器チャンネル20A,20B,20C,…,20Nは前記出力信号の処理（増巾，ろ波など）を行い、トリップ(trip)信号を作る。機器チャンネル20A,20B,20C,…,20Nはそれぞれの出力信号を導電要素22A,22B,22C,…,22N:22A′ 22B′ 22C′ ，…，22N ′ を介して一対のシリアル・リンク(serial link) 制御器24A,24Bへ供給するようになされている。また、機器チャンネル20A,…,20Nは部分トリップ信号をも生成する。本実施例では2個のシリアル・リンク制御器が用いられているが、制御システムの信頼性を高めるために2個よりも多くのシリアル・リンク制御器を使用することも同じく可能である。シリアル・リンク制御器24A,24Bはセンサ16A,16B,16C …,16Nの各々からの出力信号を、論理回路セット14A,…，14Lにそれぞれ直列に接続される導電要素26,26A′ を介して論理回路セット14A,14B,…,14Lのそれぞれにシリアルに(serially)送信するようになされている。導電要素28A,28A′ はシリアル・リンク制御器24A,24Bへ出力信号を返送し、論理回路セットが受信した出力信号が送信された出力信号と一致するかどうかの点検ができるようにする。不一致が検出されたならば、シリアル・リンク制御器は送信を停止する。シリアル信号が存在するならば、これらの信号は論理回路セットによって使用される。シリアル・リンク制御器24A,24Bは要素30A,30Bによって故障警報器（図示せず）に電気的に接続され、送

信された出力信号と論理回路セットが受信した出力信号との間の不一致がシリアル・リンク制御器24A,24Bによって検出されると、故障信号を供給して故障警報器を作動させる。

機器セット12B,12C,…,12Nも機器セット12Aと実質的に同一であり、機器セット12B,12C,…,12Nは機器セット12Aと同じパラメータを同じ位置で測定するセンサを有する。しかしながら、特定のパラメータを測定するセンサが充分に信頼度が高く、機器セットよりも少ない数しか必要ないのならば、全部のセンサを持ってはいない機器セットがあってもよい。センサが省略された場合、その出力線は、存在するセンサから所望の議決を得るための必要に応じて、トリップ状態又は非トリップ状態に結ばれる。

シリアル・リンク制御器は、例えばハミング形コーディング・スキーム（Hamming type coding scheme）又は周期的冗長性チェックなどの誤り検出コーディングなどの任意の適切なプロトコルを利用し得る。

論理回路セット14Aが第3図に詳細に図示され、各機器セット毎に1つずつ複数の自動選択論理回路32A,32B,…,32Nを具備している。自動選択論理回路32A,32B,…,32Nの各々は、シリアル信号を伴う導電要素を選択することにより、又は、シリアル信号を伴わない導電要素を回避することにより、全部のセンサからの出力信号を機器の組の1つから選択するようになされている。したがって、例えば、自動選択論理回路32Aが導電要素26A又は26A'から機器セット12Aの全部のセンサ16A,16B,16C,…,16Nからの出力信号を選択する。同様に、自動選択論理回路32Bは導電要素26B又は26B'から機器セット12Bの全部のセンサからの出力信号を選択する。同じように、自動選択論理回路32C～32Nは機器セット12C～12Nの全部のセンサからの出力信号を選択する。

ハミング形コーディング・スキームが使用されるならば、選択論理回路ではコード・チェッカーが使用される。

自動選択論理回路32A～32Nはデータ即ち選択された出力信号を同期装置36に供給するようになされている。同期装置36は、同一のパラメータを検出する各機器セットのセンサからの出力信号がそれぞれ導電要素38A～38Nを介して実質的に同時に議決論理回路40へ供給されるのを保証する。同期装置36は先入れ／先出しメモリを備える。

議決論理回路40は、同一のパラメータを検出する全ての機器セットのセンサからの出力信号に対して議決機能を遂行する。議決機能は全部の機器セットのセンサからの出力信号に対して全てのパラメータについて逐次遂行され、単一の高信頼性シリアル信号を生成する。この単一の高信頼性シリアル信号は導電要素42を介して直列－並列変換器44に供給される。直列－並列変換器44は単一の高信頼性シリアル信号を高信頼性並列信号に変換するようになされ、高信頼性並列信号は導電要素46A～46Nを介して故障停止論理回路48に供給される。

故障停止論理回路48は要素50を介して停止出力信号を供給することによって高信頼性信号に応答して停止機構の動作を制御するようになされている。

論理回路セット14B～14Lは実質的に同一であり、機器セット14Aと実質的に同一の仕方で動作する。

故障停止論理回路は2択1（one out of two）、3択2（two out of three），4択2（two out of four），4択3（three out of four）等の適切な符号の停止出力信号を出力する設計となっている。停止出力信号は要素52によって返送され、停止論理回路及び出力接続要素50を点検するために点検を受ける。この点検によって故障が検出されると、故障警報信号が電気的接続要素54によって故障警報器（図示せず）へ供給され、メンテナンスを開始するために故障警報器を動作させる。また、故障停止論理回路48は、返送点検に加え、誤り検出符号を組み入れている。

機器セット12Aは電気的コネクタ要素58A,58Bを介してシリアル・リンク制御器24A,24Bに試験信号を供給する自己試験装置56を有する。シリアル・リンク制御器24A,24Bは機器セットのセンサか

らの出力信号と共に試験信号を各論理回路セットの自動選択論理回路の1つへ順次供給する。試験信号は同期装置，議決論理回路及び直列－並列変換器によって処理される。論理回路セット14Aは直列－並列変換器44から電気的コネクター要素62によって試験信号を受信するチェッカー回路(checker circuit)64を有する。チェッカー回路64は故障警報信号を故障警報器（図示せず）に供給する電気的接続要素66を有する。

自動選択論理回路がシリアル信号の存在に基づいて判断を行うならば、故障が検出された場合にシリアル・リンク制御器が送信を停止することが必要である。

また、機器セット12B～12Nも自己試験装置を有し、論理回路セット14B～14Lもチェッカー回路を有する。

異なる機器セットの自己試験装置は異なる試験信号を送信する配置とされているので、試験信号は議決論理回路に到着するとき、1組の試験ベクトルを形成する。チェッカー回路は、議決論理回路の試験ベクトルに対する応答が並列形式への変換後に正しいことを点検し、応答が誤りであれば、故障警報信号が故障警報器へ送られ、メンテナンスを開始する。試験信号の例が3択2議決方式に対して第4図に示されている。議決論理回路は3個の機器セットの自己試験装置からの試験信号の組合せ000,011,001,…,111を順次受け取り、出力0,1,0,…，1を生成する。チェッカー回路はこれが達成されることを点検する。

制御システムは個々のパラメータ議決権(parameter voting)を有し、それぞれの個々のセンサ及びチャンネルの冗長度を適応性(flexibility)が調整できるようにする。制御システムは最も敏感な領域での故障が自己告知することができるようにする自己試験という特徴を組み込んでいる。これにより、故障検出時間を減少させてシステム故障の可能性を減らす。機器セットではなく個々のセンサ及びチャンネルでの冗長性も制御システムの故障の可能性を減少させ、きわめて信頼性の高い制御システムが生み出される。

制御システムは、従来技術におけるようなガードライン(guard line)に基づく議決権ではなく個々のパラメータで遂行される議決権を有する。制御システムの別の利点は、測定されているパラメータの数の函数ではなく必要な独立の出力信号の数の函数である論理回路セットの数で、パラメータ議決が達成されるということである。

上記の制御システムは原子炉プラント、例えば加圧水型原子炉での使用に特に適している。こうした制御システムにおいては、論理回路セットからの停止出力信号は別の制御棒又は小グループの制御棒に供給され、1本の制御棒又は小グループの制御棒の限られた作用により、1つの論理回路セット又は1本の制御棒の故障が操業停止も操業停止妨害も生じさせないようにする。

制御システムは他の方法の原子炉プラントの停止にも使いうる。

本発明が停止論理回路への言及によって説明されたが、任意の好適な制御論理回路が使用可能である。例えば、停止論理回路は、工業プラントの連続制御が停止制御よりも必要とされる場合には、制御アルゴリズム・プロセッサ回路で置換してもよい。

制御システムは、例えば危険な化学プラントのような他の工業プラントでの使用にも等しく好適である。

原子炉で使用される制御システムにおいては、センサからの出力信号はトリップ状態(trip state)であり、他の工業プラントで使用される制御システムにおいてはセンサからの出力信号はレベル(level)である。他の工業プラント用の議決論理回路はでたらめな出力信号を拒絶し、利用可能な信号の中から高信頼度・最良評価信号を生成するようになされている。

4.〔図面の簡単な説明〕

第1図は、本発明に係る工業プラント用制御システムの概略図である。

第2図は、第1図に示された機器セットの概略図である。

第3図は、第1図に示された論理回路セットの

概略図である。

第4図は、3択2議決のための試験ベクトルを示す表である。

図において、

12A～12N：機器セット

14A～14L：論理回路セット

16A～16N：センサ

20A～20N：機器チャンネル

24A～24B：シリアル・リンク制御器

32A～32N：自動選択論理回路

36：同期装置　　40：議決論理回路

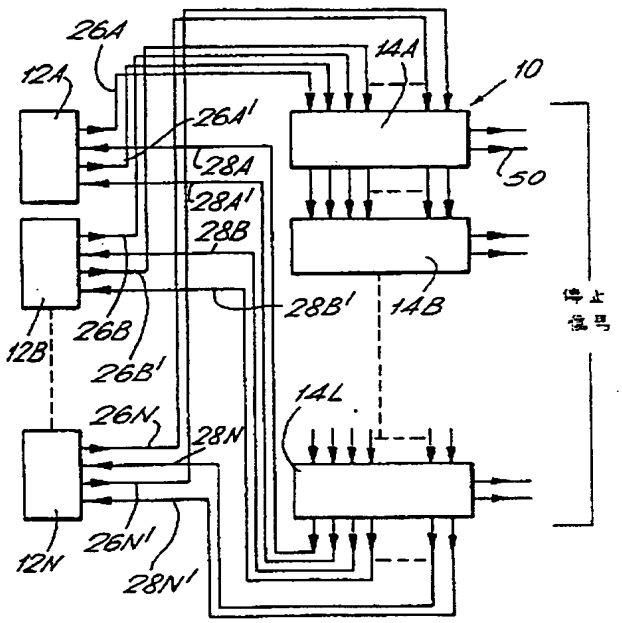
44：直列－並列変換器　48：故障停止論理回路

64：チェッカー回路

代　理　人　弁理士　湯　浅　恭　三

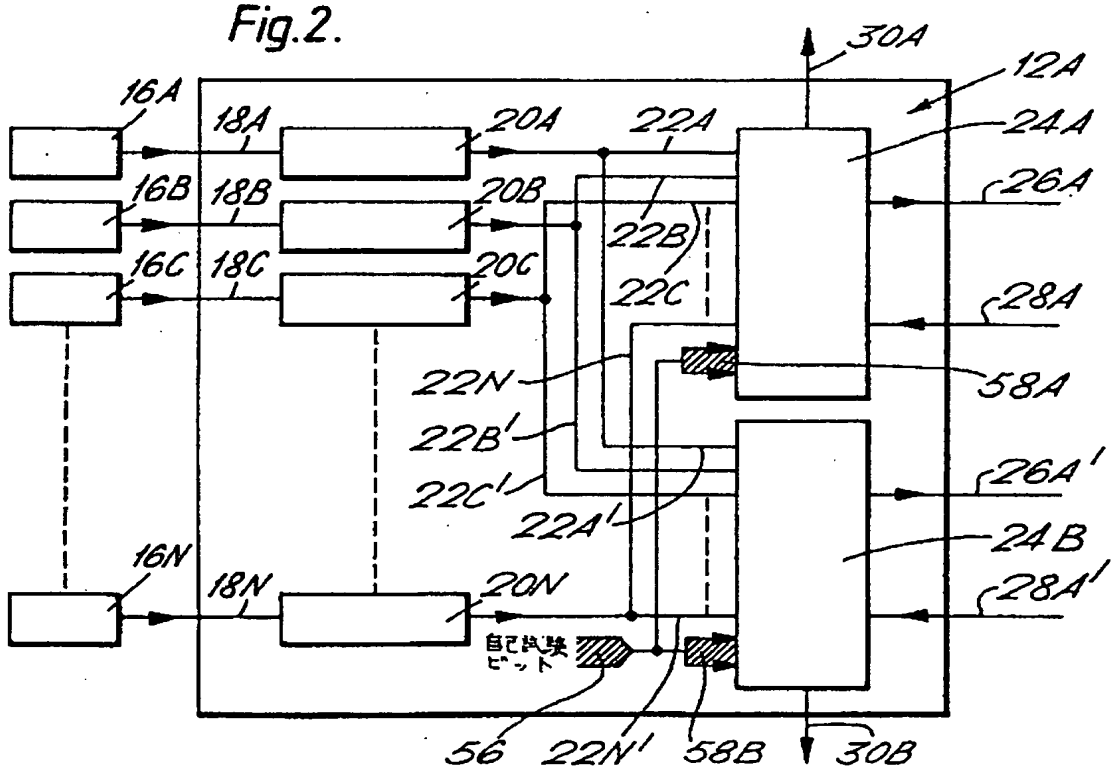
（外4名）

Fig.1.



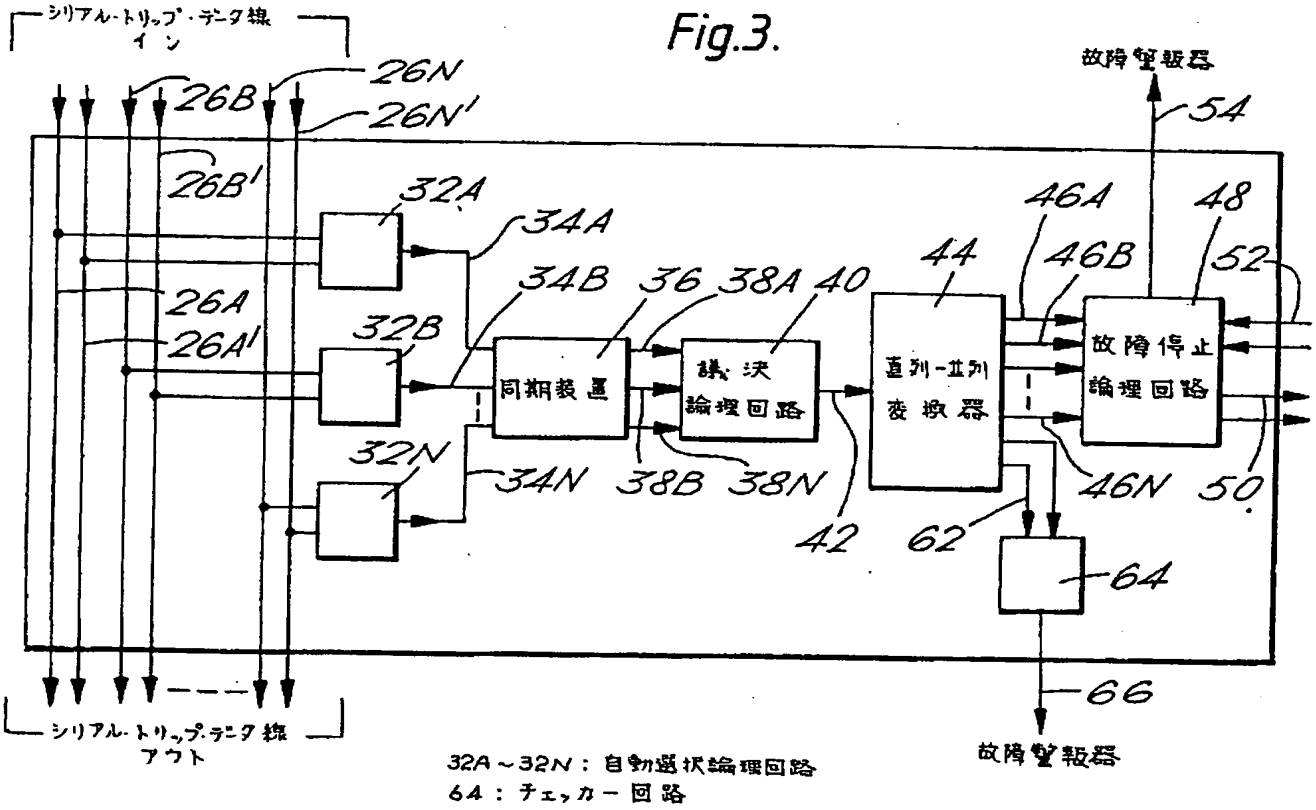
12A～12N：機器セット
14A～14L：論理回路セット

Fig.2.



16A～16N：センサ
20A～20N：機器チャンネル
24A，24B：シリアル・リンク制御器

Fig.3.



32A～32N：自動選択論理回路
64：チェッカー回路

Fig.4.

機器セット1 試験ビット	0 0 0 1 0 1 1 1
機器セット2 試験ビット	0 1 0 1 1 0 0 1
機器セット3 試験ビット	0 1 1 0 0 1 0 1
裁決装置出力	0 1 0 1 0 1 0 1